ABSTRACT

A novel and useful virtual private network (VPN) mechanism and related security association processor for maintaining the necessary security related parameters to perform security functions such as encryption, decryption and authentication. A security association database (SAD) and related circuitry is adapted to provide the necessary parameters to implement the IPSec group of security specifications for encryption/decryption and authentication. Each security association (SA) entry in the database comprises [[all]] the parameters that are necessary to receive and transmit VPN packets according to in accordance with the IPSec specification.

6